

2.2 MITIGATING SYSTEMS CORNERSTONE

The objective of this cornerstone is to monitor the availability, reliability, and capability of systems that mitigate the effects of initiating events to prevent core damage. Licensees reduce the likelihood of reactor accidents by maintaining the availability and reliability of mitigating systems. Mitigating systems include those systems associated with safety injection, decay heat removal, and their support systems, such as emergency AC power. This cornerstone includes mitigating systems that respond to both operating and shutdown events.

The definitions and guidance contained in this section, while similar to guidance developed in support of INPO/WANO indicators and the Maintenance Rule, are unique to the Reactor Oversight Process (ROP). Differences in definitions and guidance in most instances are deliberate and are necessary to meet the unique requirements of the ROP.

While safety systems are generally thought of as those that are designed to mitigate design basis accidents, not all mitigating systems have the same risk importance. PRAs have shown that risk is often influenced not only by front-line mitigating systems, but also by support systems and equipment. Such systems and equipment, both safety- and non-safety related, have been considered in selecting the performance indicators for this cornerstone. Not all aspects of licensee performance can be monitored by performance indicators, and risk-informed baseline inspections are used to supplement these indicators.

SAFETY SYSTEM FUNCTIONAL FAILURES

Purpose

This indicator monitors events or conditions that prevented, or could have prevented, the fulfillment of the safety function of structures or systems that are needed to:

- (a) Shut down the reactor and maintain it in a safe shutdown condition;
- (b) Remove residual heat;
- (c) Control the release of radioactive material; or
- (d) Mitigate the consequences of an accident.

Indicator Definition

The number of events or conditions that prevented, or could have prevented, the fulfillment of the safety function of structures or systems in the previous four quarters.

Data Reporting Elements

The following data is reported for each reactor unit:

- the number of safety system functional failures during the previous quarter

1 **Calculation**

2 unit value = number of safety system functional failures in previous four quarters

4 **Definition of Terms**

5 *Safety System Function Failure (SSFF)* is any event or condition that could have prevented the
6 fulfillment of the safety function of structures or systems that are needed to:

7
8 (A) Shut down the reactor and maintain it in a safe shutdown condition;

9 (B) Remove residual heat;

10 (C) Control the release of radioactive material; or

11 (D) Mitigate the consequences of an accident.

12
13 The indicator includes a wide variety of events or conditions, ranging from actual failures on
14 demand to potential failures attributable to various causes, including environmental qualification,
15 seismic qualification, human error, design or installation errors, etc. Many SSFFs do not involve
16 actual failures of equipment.

17
18 Because the contribution to risk of the structures and systems included in the SSFF varies
19 considerably, and because potential as well as actual failures are included, it is not possible to
20 assign a risk-significance to this indicator. It is intended to be used as a possible precursor to
21 more important equipment problems, until an indicator of safety system performance more
22 directly related to risk can be developed.

24 **Clarifying Notes**

25 *The definition of SSFFs* is identical to the wording of the current revision to 10 CFR
26 50.73(a)(2)(v). Because of overlap among various reporting requirements in 10 CFR 50.73,
27 some events or conditions that result in safety system functional failures may be properly
28 reported in accordance with other paragraphs of 10 CFR 50.73, particularly paragraphs (a)(2)(i),
29 (a)(2)(ii), and (a)(2)(vii). An event or condition that meets the requirements for reporting under
30 another paragraph of 10 CFR 50.73 should be evaluated to determine if it also prevented the
31 fulfillment of a safety function. Should this be the case, the requirements of paragraph (a)(2)(v)
32 are also met and the event or condition should be included in the quarterly performance indicator
33 report as an SSFF. The level of judgment for reporting an event or condition under paragraph
34 (a)(2)(v) as an SSFF is a reasonable expectation of preventing the fulfillment of a safety
35 function.

36
37 In the past, LERs may not have explicitly identified whether an event or condition was reportable
38 under 10 CFR 50.73(a)(2)(v) (i.e., all pertinent boxes may not have been checked). It is
39 important to ensure that the applicability of 10 CFR 50.73(a)(2)(v) has been explicitly considered
40 for each LER considered for this performance indicator.

41
42 *NUREG-1022*: Unless otherwise specified in this guideline, guidance contained in the latest
43 revision to NUREG-1022, "Event Reporting Guidelines, 10CFR 50.72 and 50.73," that is
44 applicable to reporting under 10 CFR 50.73(a)(2)(v), should be used to assess reportability for
45 this performance indicator. Questions regarding interpretation of NUREG-1022 should not be

referred to the FAQ process. They must be addressed to the appropriate NRC branch responsible for NUREG-1022.

Planned Evolution for maintenance or surveillance testing: NUREG-1022, Revision 2, page 56 states, "The following types of events or conditions generally are not reportable under these criteria:...Removal of a system or part of a system from service as part of a planned evolution for maintenance or surveillance testing..."

"Planned" means the activity is undertaken voluntarily, at the licensee's discretion, and is not required to restore operability or for continued plant operation.

A single event or condition that affects several systems: counts as only one failure.

Multiple occurrences of a system failure: the number of failures to be counted depends upon whether the system was declared operable between occurrences. If the licensee knew that the problem existed, tried to correct it, and considered the system to be operable, but the system was subsequently found to have been inoperable the entire time, multiple failures will be counted whether or not they are reported in the same LER. But if the licensee knew that a potential problem existed and declared the system inoperable, subsequent failures of the system for the same problem would not be counted as long as the system was not declared operable in the interim. Similarly, in situations where the licensee did not realize that a problem existed (and thus could not have intentionally declared the system inoperable or corrected the problem), only one failure is counted.

Additional failures: a failure leading to an evaluation in which additional failures are found is only counted as one failure; new problems found during the evaluation are not counted, even if the causes or failure modes are different. The intent is to not count additional events when problems are discovered while resolving the original problem.

Engineering analyses: events in which the licensee declared a system inoperable but an engineering analysis later determined that the system was capable of performing its safety function are not counted, even if the system was removed from service to perform the analysis.

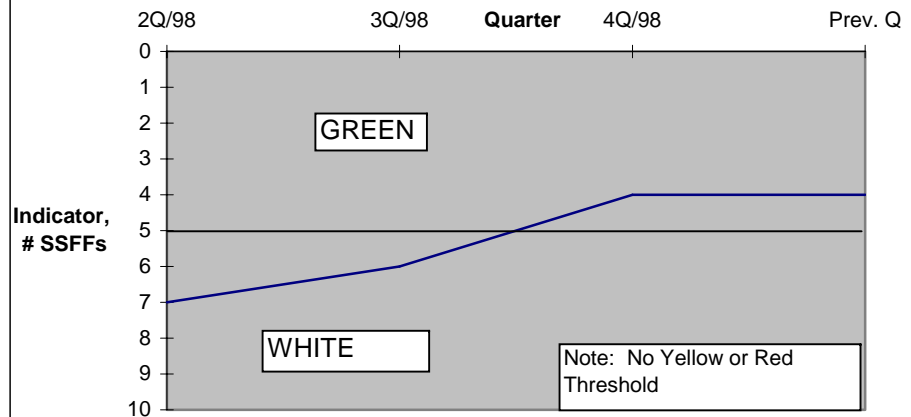
Reporting date: the date of the SSFF is the Report Date of the LER.

The LER number should be entered in the comment field when an SSFF is reported.

1 **Data Examples****Safety System Functional Failures**

Quarter	2Q/98	3Q/98	4Q/98	1Q/98	2Q/98	3Q/98	4Q/98	Prev. Q
SSFF in the previous qtr	1	3	2	1	1	2	0	1
					2Q/98	3Q/98	4Q/98	Prev. Q
Indicator: Number of SSFs over 4 Qtrs					7	6	4	4

Threshold for PWRs	
Green	≤ 5
White	> 5
Yellow	N/A
Red	N/A

Safety System Functional Failures2
3

MITIGATING SYSTEM PERFORMANCE INDEX

Purpose

The purpose of the Mitigating System Performance Index is to monitor the performance of selected systems based on their ability to perform risk-significant functions as defined herein. It is comprised of three elements - system unavailability, system unreliability and system component performance limits. The index is used to determine the cumulative significance of failures and unavailability over the monitored time period.

Indicator Definition

Mitigating System Performance Index (MSPI) is the sum of changes in a simplified core damage frequency evaluation resulting from differences in unavailability and unreliability relative to industry standard baseline values. The MSPI is supplemented with system component performance limits.

Unavailability is the ratio of the hours the train/system was unavailable to perform its monitored functions (as defined by PRA success criteria and mission times) due to planned and unplanned maintenance or test during the previous 12 quarters while critical to the number of critical hours during the previous 12 quarters. (Fault exposure hours are not included; unavailable hours are counted only from the time of discovery of a failed condition to the time the train's monitored functions are recovered.)

Unreliability is the probability that the train/system would not perform its monitored functions, as defined by PRA success criteria and mission times, when called upon during the previous 12 quarters.

Baseline values are the values for unavailability and unreliability against which current plant unavailability and unreliability are measured.

Component performance limit is a measure of degraded performance that indicates when the performance of a monitored component in an MSPI system is significantly lower than expected industry performance.

The MSPI is calculated separately for each of the following five systems for each reactor type.

BWRs

- emergency AC power system
- high pressure injection system (high pressure coolant injection, high pressure core spray, or feedwater coolant injection)
- reactor core isolation cooling(or isolation condenser)
- residual heat removal system (or the equivalent function as described in the Additional Guidance for Specific Systems section of Appendix F)
- cooling water support system (includes direct cooling functions provided by service water and component cooling water or their cooling water equivalents for the above four monitored systems)

PWRs

- emergency AC power system
- high pressure safety injection system
- auxiliary feedwater system
- residual heat removal system (or the equivalent function as described in the Additional Guidance for Specific Systems section of Appendix F)
- cooling water support system (includes direct cooling functions provided by service water and component cooling water or their cooling water equivalents for the above four monitored systems)

Data Reporting Elements

The following data elements are reported for each system

- Unavailability Index (UAI) due to unavailability for each monitored system
- Unreliability Index (URI) due to unreliability for each monitored system
- Systems that have exceeded their component performance limits

Calculation

The MSPI for each system is the sum of the UAI due to unavailability for the system plus URI due to unreliability for the system during the previous twelve quarters.

$$MSPI = UAI + URI$$

Component performance limits for each system are calculated as a maximum number of allowed failures (F_m) from the plant specific number of system demands and run hours. Actual numbers of equipment failures (F_a) are compared to these limits. This part of the indicator only applies to the green-white threshold.

See Appendix F for the calculation methodology for UAI due to system unavailability, URI due to system unreliability and system component performance limits.

The decision rules for assigning a performance color to a system are:

IF[(MSPI \leq 1.0e - 06) AND ($F_a \leq F_m$)] THEN performance is GREEN

IF{[(MSPI \leq 1.0e - 06) AND ($F_a > F_m$)] OR [(MSPI $>$ 1.0e - 06) AND (MSPI \leq 1.0e - 05)] }
THEN performance is WHITE

IF[(MSPI $>$ 1.0e - 05) AND (MSPI \leq 1.0e - 04)] THEN performance is YELLOW

IF(MSPI $>$ 1.0e - 04) THEN performance is RED

Plant Specific PRA

The MSPI calculation uses coefficients that are developed from plant specific PRAs. The PRA used to develop these coefficients should reasonably reflect the as-built, as-operated configuration of each plant. Updates to the MSPI coefficients developed from the plant specific PRA will be made as soon as practical following an update to the plant specific PRA. The revised coefficients will be used in the MSPI calculation the quarter following the update. Thus,

the PRA coefficients in use at the beginning of a quarter will remain in effect for the remainder of that quarter.

Specific requirements appropriate for this PRA application are defined in Appendix G. Any questions related to the interpretation of these requirements, the use of alternate methods to meet the requirements or the conformance of a plant specific PRA to these requirements will be arbitrated by an Industry/NRC expert panel. If the panel determines that a plant specific PRA does not meet the requirements of Appendix G such that the MSPI would be adversely affected, an appropriate remedy will be determined by the licensee and approved by the panel. The decisions of this panel will be binding.

Definition of Terms

Risk Significant Functions: those at power functions, described in the Appendix F section “Additional Guidance for Specific Systems,” that were determined to be risk-significant in accordance with NUMARC 93-01, or NRC approved equivalents (e.g., the STP exemption request). The risk significant system functions described in Appendix F, “Additional Guidance for Specific Systems” should be modeled in the plant’s PRA/PSA. System and equipment performance requirements for performing the risk significant functions are determined from the PRA success criteria for the system.

Mission Time: The mission time modeled in the PRA for satisfying the function of reaching a stable plant condition where normal shutdown cooling is sufficient. Note that PRA models typically use a mission time of 24 hours. However, shorter intervals, as justified by analyses and modeled in the PRA, may be used.

Success criteria: The plant specific values of parameters the train/system is required to achieve to perform its monitored functions. Success criteria to be used are those documented in the plant specific PRA. Design Basis success criteria should be used in the case where the plant specific PRA has not documented alternative success criteria for use in the PRA.

Individual component capability must be evaluated against train/system level success criteria (e.g., a valve stroke time may exceed an ASME requirement, but if the valve still strokes in time to meet the PRA success criteria for the train/system, the component has not failed for the purposes of this indicator.).

Clarifying Notes

Documentation

Each licensee will have the system boundaries, monitored components, and monitored functions and success criteria which differ from design basis readily available for NRC inspection on site. Design basis criteria do not need to be separately documented. Additionally, plant-specific information used in Appendix F should also be readily available for inspection. An acceptable format, listing the minimum required information, is provided in Appendix G.

Monitored Systems

Systems have been generically selected for this indicator based on their importance in preventing reactor core damage. The systems include the principal systems needed for maintaining reactor coolant inventory following a loss of coolant accident, for decay heat removal following a reactor trip or loss of main feedwater, and for providing emergency AC power following a loss

1 of plant off-site power. One support function (cooling water support system) is also monitored.
2 The cooling water support system monitors the cooling functions provided by service water and
3 component cooling water, or their direct cooling water equivalents, for the four front-line
4 monitored systems. No support systems are to be cascaded onto the monitored systems, e.g.,
5 HVAC room coolers, DC power, instrument air, etc.

6 **Diverse Systems**

7 Except as specifically stated in the indicator definition and reporting guidance, no credit is given
8 for the achievement of a monitored function by an unmonitored system in determining
9 unavailability or unreliability of the monitored systems.

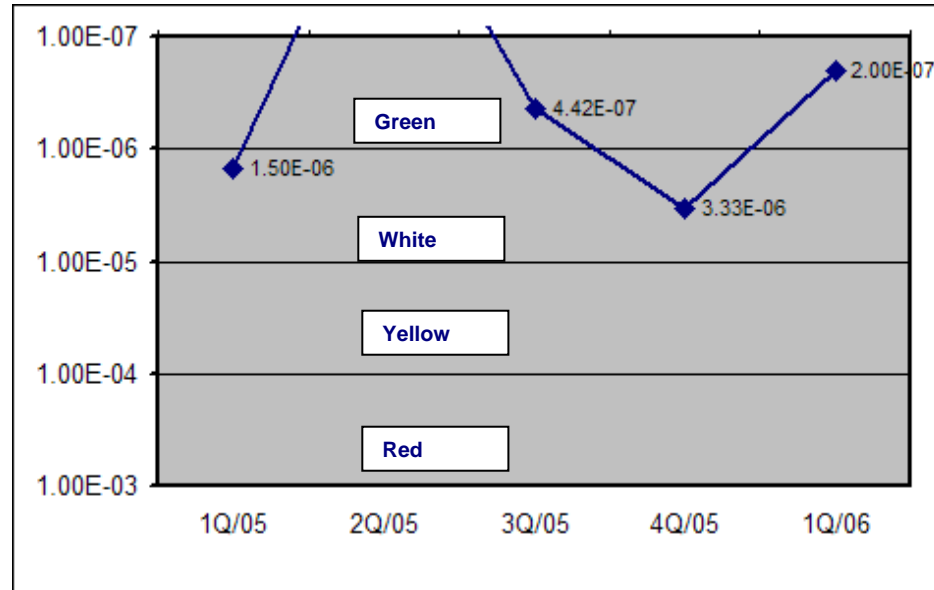
10 **Use of Plant-Specific PRA and SPAR Models**

11 The MSPI is an approximation using information from a plant's PRA and is intended as an
12 indicator of system performance. More accurate calculations using plant-specific PRAs or SPAR
13 models cannot be used to question the outcome of the PIs computed in accordance with this
14 guideline.

1 Data ExamplesMitigating System Performance Index

Quarter	1Q/05	2Q/05	3Q/05	4Q/05	1Q/06
Unavailability Index (UAI)	8.48E-08	1.00E-09	8.72E-08	1.00E-06	1.00E-07
Unreliability Index (URI)	1.42E-06	1.00E-09	3.55E-07	1.00E-06	1.00E-07
Performance Limit Exceeded	NO	NO	NO	YES	NO
Indicator Value (UAI + URI)	1.50E-06	2.00E-09	4.42E-07	PLE	2.00E-07

Threshold	
Green	$\leq 1.0\text{E-}06$
White	$> 1.0\text{E-}06$ OR PLE= Yes
Yellow	$> 1.0\text{E-}05$
Red	$> 1.0\text{E-}04$



1
2
3
4
5
6
7

[This page intentionally left blank.]